Applicants : Sydir et al.
Serial No. : 10/749,913
Filed : December 29, 2003
Page : 2 of 18

Attorney's Docket No.: INTEL-013PUS
Intel Docket No. P17940

AMENDMENTS TO THE CLAIMS:

This listing of claims replaces all prior versions and listings of claims in the application:

LISTING OF CLAIMS:

1. (Currently Amended) A processor, comprising:

a crypto unit comprising:

a cipher core configured to cipher data received;

a plurality of processing contexts each configured to process at least one data packet at a time and to store cipher keys and algorithm context associated with processing the at least one data packet, each processing context comprising authentication of the at least one packet;

authentication cores configured to authenticate the ciphered data, at least two authentication cores each implementing a different authentication algorithm; and

an authentication buffer configured to store the ciphered data and provide the ciphered data to the authentication cores each in an amount based on the corresponding authentication algorithm implemented;

Applicants : Sydir et al.
Serial No. : 10/749,913
Filed : December 29, 2003
Page : 3 of 18

Attorney's Docket No.: INTEL-013PUS
Intel Docket No. P17940

wherein the authentication buffer comprises a number of buffer elements, each buffer

element corresponding to a number respective one of the plurality of processing contexts and the

a number of the plurality of processing contexts does not equal being independent of a number of

the authentication cores.

2. (Cancelled)

3. (Previously Presented) The processor according to claim 1, wherein the plurality of

processing contexts are configured to allow latency of loading cryptographic key material and

packet data to be hidden by pipelining loading of the packet data and the key material into a first

portion of the plurality of processing contexts with processing of the packet data in a second

portion of the plurality of processing contexts.

4. (Previously Presented) The processor according to claim 1, wherein each of the buffer

elements stores data for a respective one of the processing contexts.

5. (Previously Presented) The processor according to claim 4, wherein the buffer

elements have a size that is at least as large as a largest authentication algorithm block size

implemented by the authentication cores.

Applicants : Sydir et al.
Serial No. : 10/749,913
Filed : December 29, 2003
Page : 4 of 18

Attorney's Docket No.: INTEL-013PUS
Intel Docket No. P17940

6. (Previously Presented) The processor according to claim 1, wherein the crypto unit further comprises a plurality of cipher cores configured to cipher data and the authentication buffer comprises a plurality of authentication buffer elements.

7. (Previously Presented) The processor according to claim 6, wherein the plurality of cipher cores are coupled to the authentication buffer elements via a first multiplexer device and the authentication buffer elements are coupled to the authentication cores via a second multiplexer device.

8. (Previously Presented) The processor according to claim 6, wherein one of the authentication cores processes data in 16-byte blocks and another one of the authentication cores processes data in 64-byte blocks.

9. (Previously Presented) The processor according to claim 8, wherein one of the cipher cores processes data in 8-byte blocks and another one of the cipher cores processes data in 16-byte blocks.

10. (Currently Amended) A method of cryptographic data processing, comprising:

storing ciphered data in blocks having a predetermined size;

Applicants : Sydir et al.
Serial No. : 10/749,913
Filed : December 29, 2003
Page : 5 of 18

Attorney's Docket No.: INTEL-013PUS
Intel Docket No. P17940

storing the data blocks in a first one of a plurality of buffer elements in an authentication

buffer based upon an associated one of a plurality of processing contexts, the plurality of

processing contexts each configured to process at least one data packet at a time and to store

cipher keys and algorithm context associated with processing the at least one data packet, each

processing context comprising authentication of the at least one packet; and

providing the ciphered data to authentication cores each in an amount based on a

corresponding authentication algorithm implemented by an associated authentication core, at

least two authentication cores each implementing a different authentication algorithm,

wherein the authentication buffer comprises a number of buffer elements, each buffer

element corresponding to a number respective one of the plurality of processing contexts and the

a number of the plurality of processing contexts does not equal being independent of a number of

the authentication cores.

11. (Previously Presented) The method according to claim 10, further comprising

ciphering data received in a first one of a plurality of cipher cores to form the ciphered data.

12. (Previously Presented) The method according to claim 10, further comprising

ciphering data received using a first one of a plurality of cipher algorithms to form the ciphered

data.

Applicants: Sydir et al.
Serial No. : 10/749,913
Filed : December 29, 2003
Page : 6 of 18

Attorney's Docket No.: INTEL-013PUS
Intel Docket No. P17940

13. (Previously Presented) The method according to claim 10, further comprising authenticating the ciphered data.

14. (Previously Presented) The method according to claim 10, further comprising authenticating the ciphered data using the authentication algorithms.

15. (Previously Presented) The method according to claim 10, further comprising storing the ciphered data in a first one of a plurality of buffer elements in the authentication buffer based upon an associated one of a plurality of processing contexts.

16. (Previously Presented) The method according to claim 10, further comprising the ciphering data in a plurality of cipher cores, authenticating ciphered data in a plurality of authentication cores, and processing a plurality of packets in parallel.

17. (Previously Presented) The method according to claim 10, further comprising determining whether data is to be ciphered.

18. (Currently Amended) A processor disposed on an integrated circuit, comprising:

a plurality of cipher cores;

Applicants : Sydir et al.
Serial No. : 10/749,913
Filed : December 29, 2003
Page : 7 of 18

Attorney's Docket No.: INTEL-013PUS
Intel Docket No. P17940

a plurality of processing contexts each configured to process at least one data packet at a

time and to store cipher keys and algorithm context associated with processing the at least one

data packet, each processing context comprising authentication of the at least one packet;

an authentication buffer to stored ciphered data from the plurality of cipher cores, the

authentication buffer comprising buffer elements corresponding to processing contexts, wherein

the authentication buffer is coupled to the plurality of cipher cores via a first bus; and

a plurality of authentication cores to authenticate ciphered data from the authentication

buffer, at least two authentication cores each implementing a different authentication algorithm,

wherein the authentication buffer is coupled to the plurality of authentication cores via a

second bus and configured to provide the ciphered data to the authentication cores each in an

amount based on the corresponding authentication algorithm implemented.

wherein the authentication buffer comprises a number of buffer elements, each buffer

element corresponding to a number respective one of the plurality of processing contexts and the

a number of the plurality of processing contexts not corresponding to being independent of a

number of the authentication cores.

19. (Previously Presented) The processor according to claim 18, wherein a size of at

least one of the buffer elements in the authentication buffer is at least as large as a largest

authentication algorithm block size implemented by the authentication cores.

20. (Currently Amended) A network switching device, comprising.

a processor <u>disposed on an integrated circuit</u> comprising a crypto unit comprising:

    a cipher core configured to cipher data received;

    a plurality of processing contexts each configured to process at least one data packet at a time and to store cipher keys and algorithm context associated with processing the at least one data packet<u>, each processing context comprising authentication of the at least one packet</u>;

    authentication cores configured to authenticate the ciphered data, at least two authentication cores each implementing a different authentication algorithm; and

    an authentication buffer configured to store the ciphered data and provide the ciphered data to the authentication cores each in an amount based on the corresponding authentication algorithm implemented;

    wherein the authentication buffer comprises a~~ number of~~ buffer elements<u>, each buffer element</u> corresponding to a ~~number~~ <u>respective one</u> of <u>the plurality of</u> processing contexts and ~~the~~ <u>a</u> number of <u>the plurality of</u> processing contexts <u>does not equal</u> ~~being independent of~~ a number of <u>the</u> authentication cores.

21. (Cancelled)

Applicants: Sydir et al.
Serial No. : 10/749,913
Filed : December 29, 2003
Page : 9 of 18

Attorney's Docket No.: INTEL-013PUS
Intel Docket No. P17940

22. (Previously Presented) The device according to claim 20, wherein the plurality of processing contexts are configured to allow latency of loading cryptographic key material and packet data to be hidden by pipelining loading of the packet data and the key material into a first portion of the plurality of processing contexts with processing of the packet data in a second portion of the plurality of processing contexts.

23. (Original) The device according to claim 20, wherein each of the buffer elements stores data for a respective one of the processing contexts.

24. (Original) The device according to claim 20, wherein the device includes one or more of a router, network switch, security gateway, storage area network client, and server.

25. (Currently Amended) A network, comprising.

a network switching device comprising a processor disposed on an integrated circuit comprising a crypto unit comprising:

a cipher core configured to cipher data received;

a plurality of processing contexts each configured to process at least one data packet at a time and to store cipher keys and algorithm context associated with processing the at least one data packet, each processing context comprising authentication of the at least one packet;

Applicants : Sydir et al.
Serial No. : 10/749,913
Filed : December 29, 2003
Page : 10 of 18

Attorney's Docket No.: INTEL-013PUS
Intel Docket No. P17940

authentication cores configured to authenticate the ciphered data, at least two

authentication cores each implementing a different authentication algorithm; and

an authentication buffer configured to store the ciphered data and provide the

ciphered data to the authentication cores each in an amount based on the corresponding

authentication algorithm implemented;

wherein the authentication buffer comprises a~number~of buffer elements, each buffer

element corresponding to a number respective one of the plurality of processing contexts and the

a number of the plurality of processing contexts does not equal being~independent~of a number of

the authentication cores.

26. (Cancelled)

27. (Previously Presented) The network according to claim 25, wherein the

authentication buffer includes a number of buffer elements corresponding to a number of

processing contexts are configured to allow latency of loading cryptographic key material and

packet data to be hidden by pipelining loading of the packet data and the key material into a first

portion of the plurality of processing contexts with processing of the packet data in a second

portion of the plurality of processing contexts.

Applicants : Sydir et al.
Serial No. : 10/749,913
Filed : December 29, 2003
Page : 11 of 18

Attorney's Docket No.: INTEL-013PUS
Intel Docket No. P17940

28. (Original) The network according to claim 25, wherein each of the buffer elements stores data for a respective one of the processing contexts.

29. (Original) The network according to claim 25, wherein the device includes one or more of a router, network switch, security gateway, storage area network client, and server.

30. (Previously Presented) The processor of claim 1 wherein the authentication buffer is configured to receive unciphered data.

31. (Previously Presented) The processor of claim 30 wherein the authentication buffer is configured to provide the unciphered data to one of the authentication cores in an amount based on an authentication algorithm implemented.

32. (Currently Amended) An integrated circuit chip, comprising:

a processor comprising:

cipher cores configured to cipher data received;

a plurality of processing contexts each configured to process at least one data

packet at a time and to store cipher keys and algorithm context associated with processing

the at least one data packet;

Applicants : Sydir et al.
Serial No. : 10/749,913
Filed : December 29, 2003
Page : 12 of 18

Attorney's Docket No.: INTEL-013PUS
Intel Docket No. P17940

authentication cores configured to authenticate the ciphered data, at least two

authentication cores each implementing a different authentication algorithm; and

an authentication buffer configured to store the ciphered data and provide the

ciphered data to the authentication cores each in an amount based on the corresponding

authentication algorithm implemented;

wherein the authentication buffer comprises a number of buffer elements, each buffer

element corresponding to a number respective one of the plurality of processing contexts and the

a number of the plurality of processing contexts does not equal being independent of a number of

the authentication cores.

33. (Cancelled)

34. (Previously Presented) The processor of claim 32 wherein the plurality of processing

contexts are configured to allow latency of loading cryptographic key material and packet data to

be hidden by pipelining loading of the packet data and the key material into a first portion of the

plurality of processing contexts with processing of the packet data in a second portion of the

plurality of processing contexts.

35. (Previously Presented) The processor according to claim 18, wherein the plurality of

processing contexts are configured to allow latency of loading cryptographic key material and

Applicants : Sydir et al.
Serial No. : 10/749,913
Filed : December 29, 2003
Page : 13 of 18

Attorney's Docket No.: INTEL-013PUS
Intel Docket No. P17940

packet data to be hidden by pipelining loading of the packet data and the key material into a first

portion of the plurality of processing contexts with processing of the packet data in a second

portion of the plurality of processing contexts.

36. (New) The processor of claim 6 wherein the number of the plurality of processing

contexts does not equal a number of the plurality of cipher cores.

37. (New) The processor of claim 36 wherein the number of the plurality of processing

contexts is six, a number of the buffer elements is six, the number of the plurality of cipher cores

is four and the number of the authentication cores is five.

38. (New) The processor of claim 18 wherein the number of the plurality of processing

contexts does not equal a number of the plurality of cipher cores.

39. (New) The processor of claim 38 wherein the number of the plurality of processing

contexts is six, a number of the buffer elements is six, the number of the plurality of cipher cores

is four and the number of the authentication cores is five.

40. (New) The integrated circuit chip of claim 32 wherein the number of the plurality of

processing contexts does not equal a number of the cipher cores.

Applicants : Sydir et al.
Serial No. : 10/749,913
Filed : December 29, 2003
Page : 14 of 18

Attorney's Docket No.: INTEL-013PUS
Intel Docket No. P17940

41. (New) The integrated circuit chip of claim 40 wherein the number of the plurality of processing contexts is six, a number of the buffer elements is six, the number of the cipher cores is four and the number of the authentication cores is five.